(19) 世界知识产权组织
国际局

(43) 国际公布日:
2004年5月21日(21.05.2004)

PCT

(10) 国际公布号:
WO 2004/043006 A1

(51) 国际分类号[7]: H04L 12/28

(21) 国际申请号: PCT/CN2003/000632

(22) 国际申请日: 2003年8月5日(05.08.2003)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
02139508.X 2002年11月6日(06.11.2002) CN

(71) 申请人(对除美国以外的所有指定国): 西安西电捷通无线网络通信有限公司(CHINA IWNCOMM CO., LTD) [CN/CN]; 中国陕西省西安市高新二路12号协同大厦4F.C座, Shanxi 710075 (CN)。

(72) 发明人;及

(75) 发明人/申请人(仅对美国): 铁满霞(TIE, Manxia) [CN/CN]; 唐厚俭(TANG, Houjian) [CN/CN]; 张变玲(ZHANG, Bianling) [CN/CN]; 张宁(ZHANG, Ning) [CN/CN]; 叶续茂(YE, Xumao) [CN/CN]; 中国陕西省西安市高新二路12号协同大厦4F.C座, Shanxi 710075 (CN)。

(74) 代理人: 中国专利代理(香港)有限公司(CHINA PATENT AGENT (H.K.) LTD.); 中国香港湾仔港湾道23号鹰君中心22字楼,Wanchai, Hong Kong Special Administrative Region (CN)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

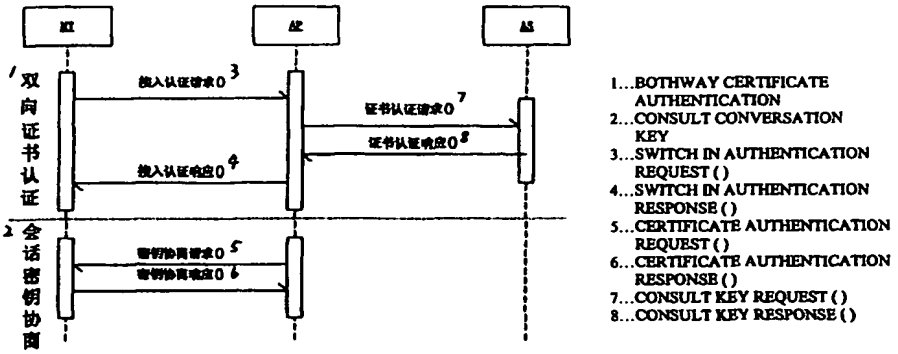
(84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A METHOD FOR THE ACCESS OF THE MOBILE TERMINAL TO THE WLAN AND FOR THE DATA COMMUNICATION VIA THE WIRELESS LINK SECURELY

(54) 发明名称: 无线局域网移动终端的安全接入与无线链路数据保密通信方法



(57) Abstract: A method for the access of the mobile terminal to the WLAN and for the data communication via the wireless link securely. Through the combination of the public key technology and the symmetrical key technology, the method can make secure access control for the mobile terminal to the WLAN and overcome the secret localization of the data communication via the wireless link. When the mobile terminal wants to enter the access point, both sides should authenticate the certificate each other. Only when both sides have the legitimate certificate, the mobile terminal can enter the access point. In order to realize the secure data communication, the mobile terminal and the access point consult the secret key for communication together, give a key for each authentication and amend the key in the conversation process. Anyhow, this method not only realizes the access control of the mobile terminal, but also ensures the security of the access control for the mobile terminal and the high privacy of the communication.

[见续页]

WO 2004/043006 A1

(57) 摘要

一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，它采用公钥密码技术和对称密码技术相结合的方式，解决了无线局域网中没有对移动终端 MT 进行有效的安全接入控制，克服了无线链路数据通信的保密局限性。当移动终端 MT 登录至无线接入点 AP 时，双方必须通过认证服务器 AS 进行双向证书认证，只有持有合法证书的移动终端 MT 才能接入持有合法证书的无线接入点 AP；移动终端 MT 与无线接入点 AP 进行会话密钥协商，完成每认证每密钥及会话过程中密钥的动态修改，以实现数据的保密通信。总之，该方法不仅完成了对移动终端 MT 的接入控制，而且保障了移动终端 MT 接入的安全性、通信的高保密性。

无线局域网移动终端的安全接入与无线链路数据保密通信方法

技术领域

本发明涉及一种无线局域网移动终端的安全接入与无线链路数据保密通信方法，它是无线通信技术与密码技术相结合的产物。

背景技术

个人通信的目标，就是使人们能够在任何时候、任何地点和其他任何人进行任意的通信联系，自由地享用网络提供的多种业务。无线局域网技术融合目前最热门的两大技术——IP 技术和无线通信技术，顺应宽带化的发展趋势，为移动主机或移动终端提供方便、高速的因特网接入服务，以适应人们对高速网络和多媒体通信业务不断增长的需求。无线局域网 WLAN（Wireless Local Area Network）不仅支持移动计算，而且具有构架的灵活性、快捷性及可扩展性。图 1 所示为以无线局域网 WLAN 为基础的宽带无线接入网络结构示意图。它主要由移动终端 MT（Mobile Terminal）、无线接入点 AP（Access Point）及无线接入服务器 WAS（Wireless Access Server）等设备组成，其中移动终端 MT 可在网中任意移动，无线接入点 AP 实现包括越区切换在内的小区管理、对移动终端 MT 的管理和桥接功能，无线接入服务器 WAS 实现移动终端 MT 的网间漫游管理。从固定接入到移动无线接入因特网，基于无线局域网 WLAN 的宽带无线 IP 技术为世界网络环境带来了全新的观念和巨大的冲击。该系统的应用非常广泛，在商务网络（主要是公司内部网）、机构用户网络（如公安、金融、政府各部门等）、小区网（如学校、医院、住宅区、远程监测或集中监控等）、临时网络（如临时会议等）、户外移动用户以及布线不易的场合、需要经常变动的场合等都非常有用。

对于无线局域网 WLAN 来说，其安全问题远比有线网严重的多，为此无线局域网 WLAN 引入了几个层次的手段来解决安全问题。首先是通过对每个无线接入点 AP 设置不同的业务组标识符 SSID

（Service Set ID），并强迫移动终端 MT 接入时提供相应的业务组标识符 SSID，从而可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。但利用业务组标识符 SSID 是最直观的一种认证方式，是较低级的安全认证，因为任何人只要知道业务组标识符 SSID 就可以接入网络。其次是地址限制，即通过在无线接入点 AP 上设置被授权的移动终端 MT 无线网卡的媒体访问控制 MAC（Medium Access Control）地址表来杜绝非授权的访问。但是无线网卡的 MAC 地址并不难获得，而且可以伪造，因此这也属于较低级别的授权认证。总之，以上两种方式都不能有效地控制移动终端 MT 的接入，更无法保障通信的保密性。

除上述两种方法外，目前更多采用的一种措施是依据无线局域网 WLAN 的国际标准（IEEE802.11），在无线局域网 WLAN 中引入基于 RC-4 的有线等价保密协议 WEP（Wired Equivalent Privacy）保密机制对数据进行加密传输。WEP 算法采用单钥体制，即加/解密使用同一密钥，其密钥长度为 64 位或 128 位。其中 40 位或 104 位为固定部分，称为初始化密钥，即在无线接入点 AP 和移动终端 MT 设置的密钥，余下的 24 位为可变部分，称为初始化矢量，该矢量在通信过程中由网卡的驱动软件来改变，也就是说用于加密的密钥可变，这在某种程度上保证了无线通信的保密性。但由于初始化矢量变化的规律性，因此 WEP 算法的安全程度并不高，这一点由美国加利福尼亚大学一研究小组最先于 2001 年 3 月发现，他们指出采用 WEP 算法的无线局域网 WLAN 仅在 5 个小时即可被攻破。其中的原因解释如下：假设初始化矢量值以每帧递增 1 的速度改变，每帧长度为 1500 字节，数据发送速率为 11 兆位/秒，则初始化矢量重复的周期为：

$$1500\text{字节}/\text{帧}\times 8\text{位}/\text{字节}\times 1\text{秒}/(11\times 10^{6}\text{位})\times 2^{24}\text{帧}\approx 18300\text{秒}\approx 5\text{小时}$$

，即每隔 5 小时就可得到经过同一密钥加密的两帧密文，由此便可猜测到或计算出初始密钥值。这里必须指出的是密钥的长度并不影响其破译的时

间，只是增加了猜测或计算的复杂度。2001 年 8 月两名以色列魏兹曼研究所的专家与一位思科公司的研究人员——三位全球顶尖译码专家进行了 WEP 安全测试，他们根据窃取网络中的一小部分资料，不到一小时即破解了无线局域网 WLAN 使用的密钥，同时 AT&T 实验室研究团体也以同样的方法成功破解，这充分说明 WEP 协议不能保障无线局域网 WLAN 的安全。安全问题已成为阻碍无线局域网 WLAN 应用普及的主要障碍之一，安全接入和保密通信也已成为无线局域网 WLAN 技术研究的重中之重。

发明内容

本发明的目的在于克服上述现有技术的不足，提供一种无线局域网移动终端的安全接入与无线链路数据保密通信方法。其采用公钥密码技术和对称密码技术相结合的方式，解决了无线局域网 WLAN 中没有对移动终端 MT 进行有效的安全接入控制，克服了无线链路数据通信保密的局限性，不仅实现了对移动终端 MT 的接入控制，而且保障了移动终端 MT 接入的安全性、通信的高保密性。

本发明提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：移动终端 MT 与无线接入点 AP 通过认证服务器 AS 进行双向证书认证；移动终端 MT 与无线接入点 AP 进行会话密钥协商。

根据本发明的优选实施例，提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，包括：当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 与无线接入点 AP 通过认证服务器 AS 进行上述双向证书认证；上述双向证书认证成功后，移动终端 MT 与无线接入点 AP 进行上述会话密钥协商。

根据本发明的优选实施例，提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，包括：当移动终端 MT 登录至无线接入点 AP 时，双方将自己的证书告知对方，接着移动

终端 MT 与无线接入点 AP 进行上述会话密钥协商；上述会话密钥协商完成后，移动终端 MT 与无线接入点 AP 通过认证服务器 AS 进行上述双向证书认证，并判断认证过程中对方使用的证书是否与对方告知的证书相同，若不同，则认证失败，若相同，则认证结果取决于上述双向证书认证过程的结果。

上述双向证书认证包括：

1）当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 向无线接入点 AP 发出含有移动终端 MT 证书的接入认证请求报文；

2）无线接入点 AP 收到上述接入认证请求报文后，在该报文中添加无线接入点 AP 证书，接着向认证服务器 AS 发出含有上述移动终端 MT 证书与无线接入点 AP 证书的证书认证请求报文；

3）认证服务器 AS 收到上述证书认证请求报文后，验证该报文中无线接入点 AP 证书和移动终端 MT 证书，然后向无线接入点 AP 返回带有认证服务器 AS 签名的证书认证响应报文；

4）无线接入点 AP 收到上述证书认证响应报文后，验证认证服务器 AS 的签名，从而得到移动终端 MT 证书的认证结果，接着将证书认证响应报文作为接入认证响应报文返回给移动终端 MT；

5）移动终端 MT 收到上述接入认证响应报文后，验证认证服务器 AS 的签名，得到无线接入点 AP 证书的认证结果，从而完成移动终端 MT 与无线接入点 AP 之间的上述双向证书认证过程。

根据本发明的优选实施例，提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，包括：1）当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 向无线接入点 AP 发出含有移动终端 MT 证书的用于上述双向证书认证的接入认证请求报文；2）无线接入点 AP 收到上述接入认证请求报文后，在该报文中添加无线接入点 AP 证书，接着向认证服务器 AS 发出含有上述移动终端 MT 证书与无线接入点 AP 证书的用于上述双向证书认证的证书认证请求报文，同时与移动终端 MT 开始会话密钥协商；3）认证服务器 AS 收到上述证书认证请求报文后，验证该报文中无线接入点 AP 证书和移动终端 MT 证书，然后向无线接入点 AP 返回带有认

证服务器 AS 签名的用于上述双向证书认证的证书认证响应报文；4）无线接入点 AP 收到上述证书认证响应报文后，验证认证服务器 AS 的签名，从而得到移动终端 MT 证书的认证结果，接着将上述证书认证响应报文作为用于上述双向证书认证的接入认证响应报文返回给移动终端 MT；5）移动终端 MT 收到上述接入认证响应报文后，验证认证服务器 AS 的签名，得到无线接入点 AP 证书的认证结果，从而完成移动终端 MT 与无线接入点 AP 之间的上述双向证书认证过程；然后移动终端 MT 进行相应的处理，完成上述会话密钥协商过程。

根据本发明的优选实施例，提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，包括：1）当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 向无线接入点 AP 发出含有移动终端 MT 证书的用于上述双向证书认证的接入认证请求报文；2）无线接入点 AP 收到上述接入认证请求报文后，在该报文中添加无线接入点 AP 证书，接着向认证服务器 AS 发出含有上述移动终端 MT 证书与无线接入点 AP 证书的用于上述双向证书认证的证书认证请求报文；3）认证服务器 AS 收到上述证书认证请求报文后，验证该报文中无线接入点 AP 证书和移动终端 MT 证书，然后向无线接入点 AP 返回带有认证服务器 AS 签名的用于上述双向证书认证的证书认证响应报文；4）无线接入点 AP 收到上述证书认证响应报文后，验证认证服务器 AS 的签名，从而得到移动终端 MT 证书的认证结果；无线接入点 AP 判断认证结果，若认证不成功，则无线接入点 AP 直接将上述证书认证响应报文作为用于上述双向证书认证的接入认证响应报文返回给移动终端 MT，若认证成功，则无线接入点 AP 向移动终端 MT 返回上述接入认证响应报文的同时与移动终端 MT 开始会话密钥协商；5）移动终端 MT 收到上述接入认证响应报文后，验证认证服务器 AS 的签名，得到无线接入点 AP 证书的认证结果，从而完成移动终端 MT 与无线接入点 AP 之间的上述双向证书认证过程；然后移动终端 MT 进行相应的处理，完成上述会话密钥协商过程。

根据本发明的优选实施例，提供了一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，包括：1）当移动终端 MT 登录至无线接入点 AP 时，双方将自己的证书告知对方，接着完成上述会话密钥协商，在此过程中移动终端 MT 还完成将接入认证请求标识告知给无线接入点 AP；2）无线接入点 AP 向认证服务器 AS 发出包括上述移动终端 MT 证书与无线接入点 AP 证书的用于上述双向证书认证的证书认证请求报文；3）认证服务器 AS 收到上述证书认证请求报文后，验证该报文中无线接入点 AP 证书和移动终端 MT 证书，然后向无线接入点 AP 返回带有认证服务器 AS 签名的用于上述双向证书认证的证书认证响应报文；4）无线接入点 AP 收到上述证书认证响应报文后，验证认证服务器 AS 的签名，从而得到移动终端 MT 证书的认证结果，接着将上述证书认证响应报文作为用于上述双向证书认证的接入认证响应报文返回给移动终端 MT；5）移动终端 MT 收到上述接入认证响应报文后，验证认证服务器 AS 的签名，接着判断该报文中无线接入点 AP 证书是否与会话密钥协商之前无线接入点 AP 告知的证书相同，若不同，则认证失败，若相同，则移动终端 MT 从该报文中得到无线接入点 AP 证书的认证结果，从而完成移动终端 MT 与无线接入点 AP 之间的上述双向证书认证过程。

上述接入认证请求报文还包括接入认证请求标识。

上述证书认证请求报文还包括接入认证请求标识或者还包括接入认证请求标识与无线接入点 AP 签名。

上述证书认证响应报文在认证服务器 AS 签名字段前还包括移动终端 MT 证书认证结果信息与无线接入点 AP 证书认证结果信息。

上述接入认证响应报文与上述证书认证响应报文相同。

上述接入认证请求标识为一串随机数据或认证序号。

上述移动终端 MT 证书认证结果信息包括移动终端 MT 证书、移动终端 MT 证书认证结果及认证服务器 AS 的签名或者包括移动终端 MT 证书与移动终端 MT 证书认证结果。

上述无线接入点 AP 证书认证结果信息包括无线接入点 AP 证

书、无线接入点 AP 证书认证结果、接入认证请求标识及认证服务器 AS 的签名或者包括无线接入点 AP 证书、无线接入点 AP 证书认证结果及接入认证请求标识。

当移动终端 MT 想接入指定的无线接入点 AP 时，该移动终端 MT 必须首先得到该无线接入点 AP 的相关信息或无线接入点 AP 的证书。

上述会话密钥协商是指移动终端 MT 或无线接入点 AP 利用无线接入点 AP 或移动终端 MT 的公钥与自己的私钥生成会话密钥。

在本发明的一个优选实施例中，上述会话密钥协商包括

1）移动终端 MT 秘密选取一个整数 a，由此计算出整数 $f(a)$，将整数 $f(a)$ 与移动终端 MT 对它的签名组成密钥协商请求报文，传给无线接入点 AP；所述的 f 为一函数，其使得由整数 $f(a)$ 得出整数 a 在计算上不可行；

2）无线接入点 AP 收到上述密钥协商请求报文后，秘密选取一个整数 b，由此计算出整数 $f(b)$，将整数 $f(b)$ 与无线接入点 AP 对它的签名组成密钥协商响应报文，传给移动终端 MT；所述的 f 为一函数，其使得由整数 $f(b)$ 得出整数 b 在计算上不可行；

3）无线接入点 AP 计算 $g(b,f(a))$，移动终端 MT 收到上述密钥协商响应报文后计算 $g(a,f(b))$，以其作为通信过程中的会话密钥；所述的 g 为一函数，其使得 $g(a,f(b))=g(b,f(a))$。

在本发明的另一个优选实施例中，上述会话密钥协商包括

1）无线接入点 AP 秘密选取一个整数 b，由此计算出整数 $f(b)$，将整数 $f(b)$ 与无线接入点 AP 对它的签名组成密钥协商请求报文，传给移动终端 MT；所述的 f 为一函数，其使得由整数 $f(b)$ 得出整数 b 在计算上不可行；

2）移动终端 MT 收到上述密钥协商请求报文后，秘密选取一个整数 a，由此计算出整数 $f(a)$，将整数 $f(a)$ 与移动终端 MT 对它的签名组成密钥协商响应报文，传给无线接入点 AP；所述的 f 为一函数，其使得由整数 $f(a)$ 得出整数 a 在计算上不可行；

3）移动终端 MT 计算 $g(a,f(b))$，无线接入点 AP 收到上述密钥协

商响应报文后计算$g(b,f(a))$，以其作为通信过程中的会话密钥；所述的g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

在本发明的另一个优选实施例中，上述会话密钥协商包括

1）移动终端 MT 或无线接入点 AP 产生一串随机数据，利用无线接入点 AP 或移动终端 MT 的公钥加密后作为密钥协商请求报文，传递给无线接入点 AP 或移动终端 MT;

2）无线接入点 AP 或移动终端 MT 收到移动终端 MT 或无线接入点 AP 发来的上述密钥协商请求报文后，利用自己的私钥进行解密，得到对方产生的随机数据；然后无线接入点 AP 或移动终端 MT 再产生一串随机数据，利用移动终端 MT 或无线接入点 AP 的公钥加密后作为密钥协商响应报文，传递给移动终端 MT 或无线接入点 AP;

3）移动终端 MT 或无线接入点 AP 收到无线接入点 AP 或移动终端 MT 发来的上述密钥协商响应报文后，利用自己的私钥进行解密，得到对方产生的随机数据；移动终端 MT 与无线接入点 AP 均利用自己与对方分别产生的随机数据生成会话密钥。

在本发明的另一个优选实施例中，上述会话密钥协商包括

1）移动终端 MT 或无线接入点 AP 产生一串随机数据，利用无线接入点 AP 或移动终端 MT 的公钥加密后，再附上自己的签名作为密钥协商请求报文，传送给无线接入点 AP 或移动终端 MT;

2）无线接入点 AP 或移动终端 MT 收到移动终端 MT 或无线接入点 AP 发来的上述密钥协商请求报文后，利用移动终端 MT 或无线接入点 AP 的公钥进行签名验证，再利用自己的私钥将收到的密文进行解密；移动终端 MT 与无线接入点 AP 均以此随机数据作为会话密钥。

此外，上述会话密钥协商还可以包括通信过程中所使用的会话算法的协商。

本发明与现有技术相比具有如下优点：

它解决了无线局域网 WLAN 中没有对移动终端 MT 进行有效的安全接入控制问题，克服了无线链路数据通信的保密局限性。它利用公钥密码体系和对称密码技术相结合的方式，实现了移动终端 MT

和无线接入点 AP 的双向证书认证，更进一步提高了接入的安全性；通过动态会话密钥协商完成每认证每密钥及会话过程中密钥的动态修改，以实现数据的保密通信，大大增加了破解的难度。总之，该方法不仅实现了对移动终端 MT 的接入控制，而且保障了移动终端 MT 接入的安全性、通信的高保密性。

附图说明

图 1 为已有技术宽带无线 IP 系统的结构示意图；

图 2 为本发明基于认证服务器 AS 的无线局域网安全认证系统的逻辑结构示意图；

图 3 为本发明移动终端 MT 接入时的认证流程图。

具体实施方式

下面将结合附图及实施例对本发明作进一步详述：

图 2 所示是基于认证服务器 AS（Authentication Server）的无线局域网安全认证系统的逻辑结构示意图。采用公钥密码技术，当移动终端 MT 登录至无线接入点 AP 时，必须利用认证服务器 AS 进行双向证书认证，只有持有合法证书的移动终端 MT 才能接入持有合法证书的无线接入点 AP，否则无线接入点 AP 拒绝移动终端 MT 接入或移动终端 MT 拒绝登录至无线接入点 AP。认证成功后，移动终端 MT 与无线接入点 AP 进行会话密钥协商，采用对称密码技术实现无线链路的数据保密通信。整个过程如图 3 所示。其中证书内容主要包含证书的序列号、证书颁发者的名称、证书的有效期、证书持有者的名称、证书持有者的公钥信息、证书颁发者采用的签名算法以及证书颁发者对证书的签名等内容。

1、双向证书认证

当移动终端 MT 登录至无线接入点 AP 时，双方通过认证服务器 AS 进行双向证书认证，流程如下：

a)接入认证请求。移动终端 MT 向无线接入点 AP 发出接入认证请求报文，即将移动终端 MT 证书与一串随机数据或认证序号发往无线接入点 AP，其中随机数据串或认证序号被称为接入认证请求标识；

b)证书认证请求。无线接入点 AP 收到移动终端 MT 接入认证请求报文后，向认证服务器 AS 发出证书认证请求报文，即将移动终端 MT 证书、接入认证请求标识及无线接入点 AP 证书或者将移动终端 MT 证书、接入认证请求标识、无线接入点 AP 证书及用无线接入点 AP 的私钥对它们的签名构成证书认证请求报文，发送给认证服务器 AS;

c)证书认证响应。认证服务器 AS 收到无线接入点 AP 的证书认证请求报文后，若该报文中带有无线接入点 AP 的签名，则先验证签名的正确性，若不正确，则将认证结果置为失败。接着验证无线接入点 AP 证书和移动终端 MT 证书的合法性。验证完毕，认证服务器 AS 将[1].移动终端 MT 证书认证结果信息包括移动终端 MT 证书及移动终端 MT 证书认证结果及认证服务器 AS 对它们的签名或者仅包括移动终端 MT 证书及移动终端 MT 证书认证结果，[2].无线接入点 AP 证书认证结果信息包括无线接入点 AP 证书及无线接入点 AP 证书认证结果及接入认证请求标识及认证服务器 AS 对它们的签名或者仅包括无线接入点 AP 证书及无线接入点 AP 证书认证结果及接入认证请求标识，[3].认证服务器 AS 对[1]和[2]的签名构成证书认证响应报文，发回给无线接入点 AP;

d)接入认证响应。无线接入点 AP 对认证服务器 AS 返回的证书认证响应报文的签名进行验证，便得到移动终端 MT 证书的认证结果。无线接入点 AP 将证书认证响应报文作为接入认证响应报文，回送至移动终端 MT;

e)移动终端 MT 对无线接入点 AP 返回的接入认证响应报文的签名进行验证，便得到无线接入点 AP 证书的认证结果。

至此移动终端 MT 与无线接入点 AP 之间完成了双向证书认证过程。若双方证书验证成功，则无线接入点 AP 允许移动终端 MT 接入，否则拒绝其接入或者移动终端 MT 拒绝登录到无线接入点 AP。至此，具有合法证书的移动终端 MT 才成功地接入具有合法证书的无线接入点 AP，从而完成无线接入点 AP 对移动终端 MT 的安全接入控制功能。

2、会话密钥协商

移动终端 MT 与无线接入点 AP 双向证书认证成功之后，即完成了移动终端 MT 的成功登录。此时双方在本机利用对方的公钥与自己的私钥生成会话密钥，用于通信数据报文的加解密，从而实现移动终端 MT 与无线接入点 AP 之间的无线安全保密通信。然而值得注意的是，在证书有效期内，移动终端 MT 与无线接入点 AP 之间的会话密钥始终不变。为了做到每认证每密钥，则需进行会话密钥的动态协商。动态会话密钥协商的过程如下：

a) 密钥协商请求。移动终端 MT 或无线接入点 AP 产生一串随机数据，利用无线接入点 AP 或移动终端 MT 的公钥加密后，向无线接入点 AP 或移动终端 MT 发出密钥协商请求报文；

b) 密钥协商响应。无线接入点 AP 或移动终端 MT 收到移动终端 MT 或无线接入点 AP 发来的密钥协商请求报文后，利用自己的私钥进行解密，得到对方产生的随机数据。然后本地产生一串随机数据，利用移动终端 MT 或无线接入点 AP 的公钥加密后，向移动终端 MT 或无线接入点 AP 回应密钥协商响应报文；

c) 移动终端 MT 或无线接入点 AP 收到无线接入点 AP 或移动终端 MT 发来的密钥协商响应报文后，利用自己的私钥进行解密，得到对方产生的随机数据；移动终端 MT 与无线接入点 AP 均在利用自己与对方分别产生的两个随机数据生成会话密钥，用于对通信数据报文的加解密。

为了进一步提高通信的保密性，在移动终端 MT 与无线接入点 AP 通信一段时间或交换一定数量的报文之后，还可以进行会话密钥的重新协商。

双向证书认证完成了移动终端 MT 的安全接入，会话密钥协商则充分保证了移动终端 MT 与无线接入点 AP 之间的高保密性通信。

特别指出的是：

（1）若移动终端 MT 欲接入指定的无线接入点 AP，则在双向证书认证之前移动终端 MT 应知晓该无线接入点 AP 的相关信息或存有该无线接入点 AP 的证书，以便移动终端 MT 对接收到的接入认证响应

报文进行判断。

（2）会话密钥协商还可以包括会话算法的协商，即在会话密钥协商请求报文中罗列出请求方所支持的会话算法，响应方在请求方提供的会话算法中选择一种，通过会话密钥协商响应报文传回给请求方。会话密钥协商完成后，双方采用协商的会话算法进行保密通信。

（3）会话密钥的动态协商还可以如下实现，即移动终端 MT 或无线接入点 AP 在本地产生一串随机数据，利用对方的公钥加密后再附上自己的签名传送给对方，无线接入点 AP 或移动终端 MT 收到后，利用对方的公钥验证是否是对方发送的数据，然后再利用自己的私钥将收到的密文进行解密，双方将此随机数据作为会话密钥对通信数据进行加解密。

（4）会话密钥协商还可如下进行:

a)移动终端 MT 秘密选取一个整数a，计算出$f(a)$，将$f(a)$与移动终端 MT 对此的签名传给无线接入点 AP。其中f为一函数，使得由$f(a)$得出a在计算上是不可行的;

b)无线接入点 AP 秘密选取一个整数b，计算出$f(b)$，将$f(b)$与无线接入点 AP 对此的签名传给移动终端 MT。其中f函数的定义同 a);

c)移动终端 MT 计算$g(a,f(b))$，无线接入点 AP 计算$g(b,f(a))$，作为通信过程中的会话密钥。其中g为一函数，使得$g(a,f(b))=g(b,f(a))$。

（5）前面所述的是先进行双向证书认证再进行会话密钥协商，但在具体实现过程中，还可以先进行会话密钥协商再进行双向证书认证，或者将两个过程合并或交叉进行。

（6）先进行会话密钥协商后进行双向证书认证的具体实现如下:

a)当移动终端 MT 登录至无线接入点 AP 时，双方将自己的证书告知对方;

b)采用如前所述的方法，移动终端 MT 与无线接入点 AP 进行会话密钥协商;

c)采用如前所述的方法，移动终端 MT 与无线接入点 AP 进行双向证书认证，并判断对方使用的证书是否与 a)步骤中对方告知的证

书相同，若不同，则认证失败；否则认证结果取决于双向证书认证过程的结果。

（7）双向证书认证与会话密钥协商的交叉实现如下：

双向证书认证与会话密钥协商过程完全同前，只是将报文的顺序进行了交叉。即当移动终端 MT 登录至无线接入点 AP 时，移动终端 MT 向无线接入点 AP 发出接入认证请求报文，无线接入点 AP 收到该报文后，向认证服务器 AS 发出证书认证请求报文的同时与移动终端 MT 开始会话密钥协商。从而双向证书认证与会话密钥协商交叉完成，它相比分离实现，速度加快。

（8）双向证书认证与会话密钥协商的合并实现如下：

当移动终端 MT 登录至无线接入点 AP 时，双方先进行双向证书认证再进行会话密钥协商，但在认证过程即将结束时，即无线接入点 AP 向移动终端 MT 返回接入认证响应报文的同时开始与移动终端 MT 进行会话密钥协商，即可以在接入认证响应报文中添加密钥协商请求信息。从而双向证书认证与会话密钥协商部分合并完成，它相比分离实现，速度加快。

（9）双向证书认证与会话密钥协商还可如下实现，即对先会话密钥协商后双向证书认证的实现方法进行简化。在移动终端 MT 和无线接入点 AP 将自己的证书告知对方和会话密钥协商的过程中，移动终端 MT 还应完成将接入认证请求标识告知给无线接入点 AP，因此接着进行双向证书认证时，移动终端 MT 不需向无线接入点 AP 发送接入认证请求报文，而是由无线接入点 AP 直接向认证服务器 AS 发出证书认证请求报文开始双向证书认证，该认证过程结束时仅需移动终端 MT 判断无线接入点 AP 所使用的证书是否与会话密钥协商之前无线接入点 AP 告知的证书相同，若不同，则认证失败，若相同，认证结果取决于双向证书认证过程的结果。

权 利 要 求

1. 一种用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：移动终端（MT）与无线接入点（AP）通过认证服务器（AS）进行双向证书认证；移动终端（MT）与无线接入点（AP）进行会话密钥协商。

2. 根据权利要求 1 所述的用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：

当移动终端（MT）登录至无线接入点（AP）时，移动终端（MT）与无线接入点（AP）通过认证服务器（AS）进行所述双向证书认证；

所述双向证书认证成功后，移动终端（MT）与无线接入点（AP）进行所述会话密钥协商。

3. 根据权利要求 1 所述的用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：

当移动终端（MT）登录至无线接入点（AP）时，双方将自己的证书告知对方，接着移动终端（MT）与无线接入点（AP）进行所述会话密钥协商；

所述会话密钥协商完成后，移动终端（MT）与无线接入点（AP）通过认证服务器（AS）进行所述双向证书认证，同时判断认证过程中对方使用的证书是否与对方告知的证书相同，若不同，则认证失败；若相同，则认证结果取决于所述双向证书认证过程的结果。

4. 根据权利要求 1、2 或 3 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的双向证书认证包括步骤：

1）. 当移动终端（MT）登录至无线接入点（AP）时，移动终端（MT）向无线接入点（AP）发出含有移动终端（MT）证书的接入认证请求报文；

2）. 无线接入点（AP）收到所述接入认证请求报文后，在该报文中添加无线接入点（AP）证书，接着向认证服务器（AS）发出包括所述移动终端（MT）证书与无线接入点（AP）证书的证书认证请

求报文;

3）.认证服务器（AS）收到所述证书认证请求报文后，验证该报文中无线接入点（AP）证书和移动终端（MT）证书，然后向无线接入点（AP）返回带有认证服务器（AS）签名的证书认证响应报文;

4）.无线接入点（AP）收到所述证书认证响应报文后，验证认证服务器（AS）的签名，从而得到移动终端（MT）证书的认证结果，接着将所述证书认证响应报文作为接入认证响应报文返回给移动终端（MT）;

5）.移动终端（MT）收到所述接入认证响应报文后，验证认证服务器（AS）的签名，得到无线接入点（AP）证书的认证结果，从而完成移动终端（MT）与无线接入点（AP）之间的所述双向证书认证过程。

5. 根据权利要求 1 所述的用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于:

1）.当移动终端（MT）登录至无线接入点（AP）时，移动终端（MT）向无线接入点（AP）发出含有移动终端（MT）证书的用于所述双向证书认证的接入认证请求报文;

2）.无线接入点（AP）收到所述接入认证请求报文后，在该报文中添加无线接入点（AP）证书，接着向认证服务器（AS）发出含有所述移动终端（MT）证书与无线接入点（AP）证书的用于所述双向证书认证的证书认证请求报文，同时与移动终端（MT）开始会话密钥协商;

3）.认证服务器（AS）收到所述证书认证请求报文后，验证该报文中无线接入点（AP）证书和移动终端（MT）证书，然后向无线接入点（AP）返回带有认证服务器（AS）签名的用于所述双向证书认证的证书认证响应报文;

4）.无线接入点（AP）收到所述证书认证响应报文后，验证认证服务器（AS）的签名，从而得到移动终端（MT）证书的认证结果，接着将所述证书认证响应报文作为用于所述双向证书认证的接入认证响应报文返回给移动终端（MT）;

5）.移动终端（MT）收到所述接入认证响应报文后，验证认证服务器（AS）的签名，得到无线接入点（AP）证书的认证结果，从而完成移动终端（MT）与无线接入点（AP）之间的所述双向证书认证过程；然后移动终端（MT）进行相应的处理，完成所述会话密钥协商过程。

6.根据权利要求 1 所述的用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：

1）.当移动终端（MT）登录至无线接入点（AP）时，移动终端（MT）向无线接入点（AP）发出含有移动终端（MT）证书的用于所述双向证书认证的接入认证请求报文；

2）.无线接入点（AP）收到所述接入认证请求报文后，在该报文中添加无线接入点（AP）证书，接着向认证服务器（AS）发出含有所述移动终端（MT）证书与无线接入点（AP）证书的用于所述双向证书认证的证书认证请求报文；

3）.认证服务器（AS）收到所述证书认证请求报文后，验证该报文中无线接入点（AP）证书和移动终端（MT）证书，然后向无线接入点（AP）返回带有认证服务器（AS）签名的用于所述双向证书认证的证书认证响应报文；

4）.无线接入点（AP）收到所述证书认证响应报文后，验证认证服务器（AS）的签名，从而得到移动终端（MT）证书的认证结果；无线接入点（AP）判断认证结果，若认证不成功，则无线接入点（AP）直接将所述证书认证响应报文作为用于所述双向证书认证的接入认证响应报文返回给移动终端（MT），若认证成功，则无线接入点（AP）向移动终端（MT）返回所述接入认证响应报文的同时与移动终端（MT）开始所述会话密钥协商；

5）.移动终端（MT）收到所述接入认证响应报文后，验证认证服务器（AS）的签名，得到无线接入点（AP）证书的认证结果，从而完成移动终端（MT）与无线接入点（AP）之间的所述双向证书认证过程；然后移动终端（MT）进行相应的处理，完成所述会话密钥协商过程。

7. 根据权利要求 1 所述的用于无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：

1）.当移动终端（MT）登录至无线接入点（AP）时，双方将自己的证书告知对方，接着完成所述会话密钥协商，在此过程中移动终端（MT）还完成将接入认证请求标识告知给无线接入点（AP）；

2）.无线接入点（AP）向认证服务器（AS）发出包括所述移动终端（MT）证书与无线接入点（AP）证书的用于所述双向证书认证的证书认证请求报文；

3）.认证服务器（AS）收到所述证书认证请求报文后，验证该报文中无线接入点（AP）证书和移动终端（MT）证书，然后向无线接入点（AP）返回带有认证服务器（AS）签名的用于所述双向证书认证的证书认证响应报文；

4）.无线接入点（AP）收到所述证书认证响应报文后，验证认证服务器（AS）的签名，从而得到移动终端（MT）证书的认证结果，接着将所述证书认证响应报文作为用于所述双向证书认证的接入认证响应报文返回给移动终端（MT）；

5）.移动终端（MT）收到所述接入认证响应报文后，验证认证服务器（AS）的签名，接着判断该报文中无线接入点（AP）证书是否与会话密钥协商之前无线接入点（AP）告知的证书相同，若不同，则认证失败，若相同，则移动终端（MT）从该报文中得到无线接入点（AP）证书的认证结果，从而完成移动终端（MT）与无线接入点（AP）之间的所述双向证书认证过程。

8. 根据权利要求 4、5 或 6 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的接入认证请求报文还包括接入认证请求标识。

9. 根据权利要求 4、5、6 或 7 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的证书认证请求报文还包括接入认证请求标识或者还包括接入认证请求标识与无线接入点 AP 签名。

10. 根据权利要求 4、5、6 或 7 所述的无线局域网移动终端的

安全接入与无线链路数据保密通信方法，其特征在于：所述的证书认证响应报文在认证服务器（AS）签名字段前还包括移动终端（MT）证书认证结果信息与无线接入点（AP）证书认证结果信息。

11. 根据权利要求 4、5、6 或 7 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的接入认证响应报文与所述的证书认证响应报文相同。

12. 根据权利要求 7、8 或 9 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的接入认证请求标识为一串随机数据或认证序号。

13. 根据权利要求 10 或 11 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的移动终端（MT）证书认证结果信息包括移动终端（MT）证书、移动终端（MT）证书认证结果及认证服务器（AS）的签名或者包括移动终端（MT）证书与移动终端（MT）证书认证结果。

14. 根据权利要求 10 或 11 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的无线接入点（AP）证书认证结果信息包括无线接入点（AP）证书、无线接入点（AP）证书认证结果、接入认证请求标识及认证服务器（AS）的签名或者包括无线接入点（AP）证书、无线接入点（AP）证书认证结果及接入认证请求标识。

15. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终端的安全接入和无线链路数据保密通信方法，其特征在于：当移动终端（MT）想接入指定的无线接入点（AP）时，该移动终端（MT）必须首先得到该无线接入点（AP）的相关信息或无线接入点（AP）的证书。

16. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的会话密钥协商是指移动终端（MT）或无线接入点（AP）利用无线接入点（AP）或移动终端（MT）的公钥与自己的私钥生成会话密钥。

17. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终

端的安全接入和无线链路数据保密通信方法，其特征在于：所述的会话密钥协商包括

1）.移动终端（MT）秘密选取一个整数a，由此计算出整数$f(a)$，将整数$f(a)$与移动终端（MT）对它的签名组成密钥协商请求报文，传给无线接入点（AP）；所述的f为一函数，其使得由整数$f(a)$得出整数a在计算上不可行；

2）.无线接入点（AP）收到所述密钥协商请求报文后，秘密选取一个整数b，由此计算出整数$f(b)$，将整数$f(b)$与无线接入点（AP）对它的签名组成密钥协商响应报文，传给移动终端（MT）；所述的f为一函数，其使得由整数$f(b)$得出整数b在计算上不可行；

3）. 无线接入点（AP）计算$g(b,f(a))$，移动终端（MT）收到所述密钥协商响应报文后计算$g(a,f(b))$，以其作为通信过程中的会话密钥；所述的g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

18. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终端的安全接入和无线链路数据保密通信方法，其特征在于：所述的会话密钥协商包括

1）.无线接入点（AP）秘密选取一个整数b，由此计算出整数$f(b)$，将整数$f(b)$与无线接入点（AP）对它的签名组成密钥协商请求报文，传给移动终端（MT）；所述的f为一函数，其使得由整数$f(b)$得出整数b在计算上不可行；

2）.移动终端（MT）收到所述密钥协商请求报文后，秘密选取一个整数a，由此计算出整数$f(a)$，将整数$f(a)$与移动终端（MT）对它的签名组成密钥协商响应报文，传给无线接入点（AP）；所述的f为一函数，其使得由整数$f(a)$得出整数a在计算上不可行；

3）.移动终端（MT）计算$g(a,f(b))$，无线接入点（AP）收到所述密钥协商响应报文后计算$g(b,f(a))$，以其作为通信过程中的会话密钥；所述的g为一函数，其使得$g(a,f(b))=g(b,f(a))$。

19. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的会话密钥协商包括

1）.移动终端（MT）或无线接入点（AP）产生一串随机数据，利用无线接入点（AP）或移动终端（MT）的公钥加密后作为密钥协商请求报文，传递给无线接入点（AP）或移动终端（MT）；

2）.无线接入点（AP）或移动终端（MT）收到移动终端（MT）或无线接入点（AP）发来的所述密钥协商请求报文后，利用自己的私钥进行解密，得到对方产生的随机数据；然后无线接入点（AP）或移动终端（MT）再产生一串随机数据，利用移动终端（MT）或无线接入点（AP）的公钥加密后作为密钥协商响应报文，传递给移动终端（MT）或无线接入点（AP）；

3）.移动终端（MT）或无线接入点（AP）收到无线接入点（AP）或移动终端（MT）发来的所述密钥协商响应报文后，利用自己的私钥进行解密，得到对方产生的随机数据；移动终端（MT）与无线接入点（AP）均利用自己与对方分别产生的随机数据生成会话密钥。

20. 如权利要求 1、2、3、5、6 或 7 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的会话密钥协商包括

1）.移动终端（MT）或无线接入点（AP）产生一串随机数据，利用无线接入点（AP）或移动终端（MT）的公钥加密后，再附上自己的签名作为密钥协商请求报文，传送给无线接入点（AP）或移动终端（MT）；

2）.无线接入点（AP）或移动终端（MT）收到移动终端（MT）或无线接入点（AP）发来的所述密钥协商请求报文后，利用移动终端（MT）或无线接入点（AP）的公钥进行签名验证，再利用自己的私钥将收到的密文进行解密；移动终端 MT 与无线接入点 AP 均以此随机数据作为会话密钥。

21. 如权利要求 17、18 或 19 所述的无线局域网移动终端的安全接入与无线链路数据保密通信方法，其特征在于：所述的会话密钥协商还可以包括通信过程中所使用的会话算法的协商。

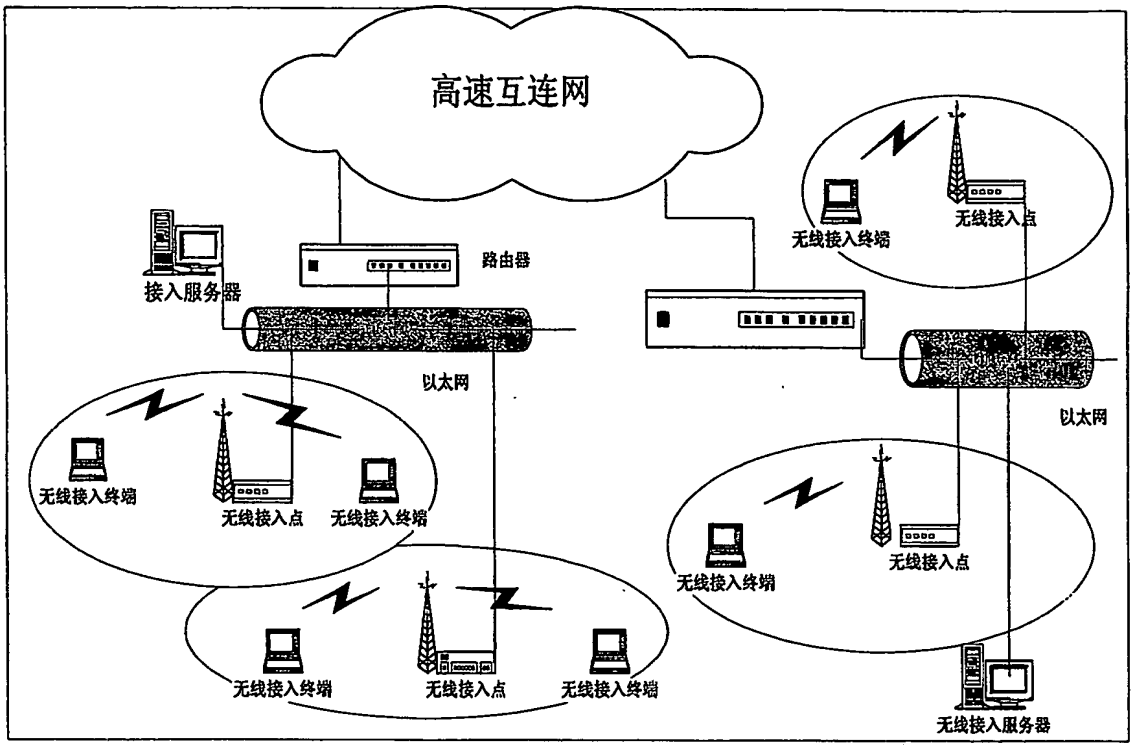

高速互连网
接入服务器
路由器
以太网
无线接入终端
无线接入点
无线接入终端
无线接入终端
无线接入点
以太网
无线接入终端
无线接入点
无线接入终端
无线接入终端
无线接入点
无线接入终端
无线接入服务器

图 1

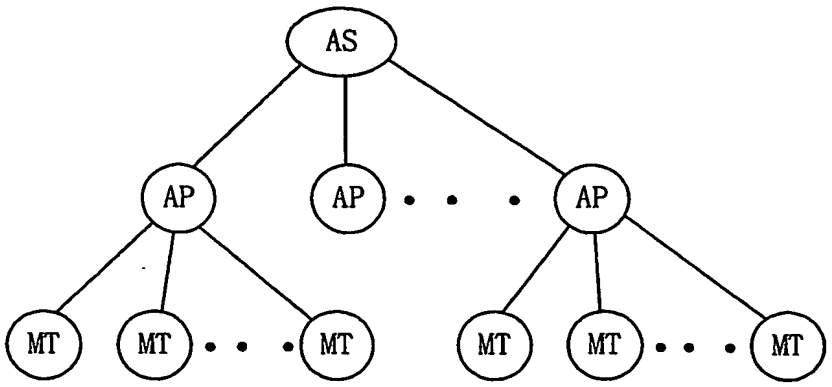

AS
AP
AP
AP
MT
MT
MT
MT
MT
MT

图 2

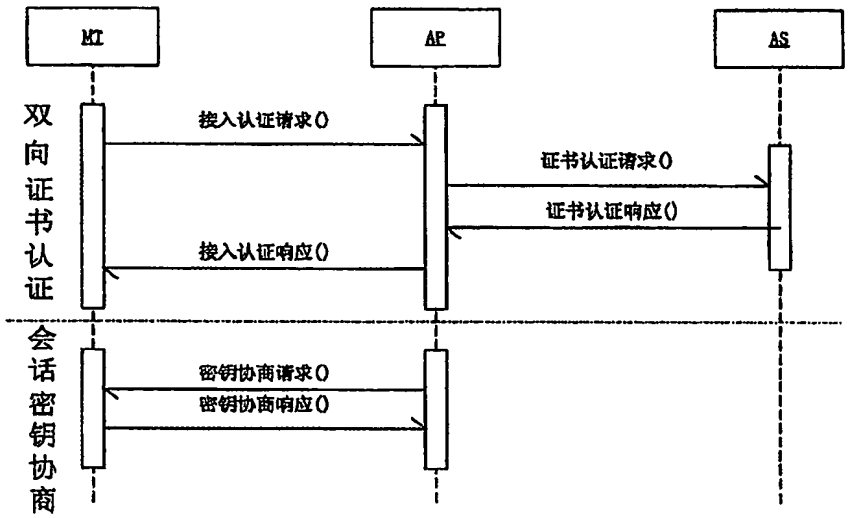

MT
AP
AS
双向证书认证
接入认证请求()
证书认证请求()
证书认证响应()
接入认证响应()
会话密钥协商
密钥协商请求()
密钥协商响应()

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN03/00632

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 H04L12/28 H04L9/32 H04L9/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN,A,1249587(LUCENT TECHNOLOGIES INC)5.April 2000, see the whole document ,figure 3	1-21
A	CN,A,1316147(SAMSUNG ELECTRONICS CO LTD)3.October 2001, see the whole document ,figure 3	1-21
A	US,B1, 6229806 (MOTOROLA INC)8.May 2001, see the whole document ,figure 1、2	1-21
A	WO,A1,0209345(GEMPLUS)1.January 2002, see the whole document	1-21
A	EP,A2,1098489(NOKIA CORP)9.May 2001, see the whole document ,figure 4、6	1-21
A	JP,A,2001285956(TOSHIBA CORP)12. October 2001, see the whole document ,figure 1、8	1-21

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
18. Sep.2003 (18.09.03)

Date of mailing of the international search report
23 OCT 2003 (23.10.03)

Name and mailing address of the ISA/CN
6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China
Facsimile No. 86-10-62019451

Authorized officer
HU,Xiangli
Telephone No: 86-10-82755422

Form PCT/ISA /210 (second sheet) (July 1998)

Form PCT/ISA /210 (continuation of Second sheet (2)) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN03/00632

Patent document Cited in search report	Publication date	Patent family member(s)	Publication date
CN1249587A	05.04.00	KR2000012072A	25.02.00
		BR9902804A	28.03.00
		JP2000106553A	11.04.00
		EP0998095A	03.05.00
		TW429721B	11.04.01
CN1316147A	03.10.01	NONE	
US6229806B1	08.05.01	NONE	
WO0209345A	31.01.02	FR2812509A1	01.02.02
		AU7853901A	05.02.02
		EP1307994A1	07.05.03
EP1098489A2	09.05.01	JP2001204055A	27.07.01
JP2001285956A	12.10.01	JP2003101780A	04.04.03

国际检索报告

国际申请号
PCT/CN03/00632

A. 主题的分类

IPC7 H04L12/28

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类体系和分类号)

IPC7 H04L12/28 H04L9/32 H04L9/14

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称和，如果实际可行的，使用的检索词)

WPI，EPODOC，PAJ，CNPAT

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求编号
A	CN,A,1249587(朗讯科技公司)2000 年 4 月 5 日(05.04.00),说明书全文,图 3	1-21
A	CN,A,1316147(三星电子株式会社)2001 年 10 月 3 日(03.10.01),说明书全文,图 3	1-21
A	US,B1, 6229806 (MOTOROLA INC)2001 年 5 月 8 日(08.05.01),说明书全文,图 1、2	1-21
A	WO,A1,0209345(GEMPLUS)2002 年 1 月 31 日(31.01.02),说明书全文	1-21
A	EP,A2,1098489(NOKIA CORP)2001 年 5 月 9 日(09.05.01),说明书全文,图 4、6	1-21
A	JP,A,2001285956(TOSHIBA CORP)2001 年 10 月 12 日(12.10.01)，说明书全文，图 1、8	1-21

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的专用类型：

"A" 明确叙述了被认为不是特别相关的一般现有技术的文件

"E" 在国际申请日的当天或之后公布的在先的申请或专利

"L" 可能引起对优先权要求的怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布的在后文件，它与申请不相抵触，但是引用它是为了理解构成发明基础的理论或原理

"X" 特别相关的文件，仅仅考虑该文件，权利要求所记载的发明就不能认为是新颖的或不能认为是有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，权利要求记载的发明不具有创造性

"&" 同族专利成员的文件

国际检索实际完成的日期	国际检索报告邮寄日期
18.9 月 2003(18.09.03)	23. 10月 2003 (23.10.03)
国际检索单位名称和邮寄地址 ISA/CN 中国北京市海淀区西土城路 6 号(100088) 传真号： 86-10-62019451	受权官员 胡向莉 电话号码：86-10-82755422

国际检索报告

关于同族专利成员的情报

国际申请号
PCT/CN03/00632

检索报告中引用的专利文件	公布日期	同族专利成员	公布日期
CN1249587A	05.04.00	KR2000012072A	25.02.00
		BR9902804A	28.03.00
		JP2000106553A	11.04.00
		EP0998095A	03.05.00
		TW429721B	11.04.01
CN1316147A	03.10.01	无	
US6229806B1	08.05.01	无	
WO0209345A1	31.01.02	FR2812509A1	01.02.02
		AU7853901A	05.02.02
		EP1307994A1	07.05.03
EP1098489A2	09.05.01	JP2001204055A	27.07.01
JP2001285956A	12.10.01	JP2003101780A	04.04.03